

CLAIMS

1. An apparatus comprising:
 - a first encryption key storage unit configured to store a first encryption key;
 - a second encryption key storage unit configured to contain a second encryption key;
 - an encryption unit configured to encrypt a message containing a first encryption key, the message encrypted with the second encryption key;
 - a radio configured to transmit the message over a wireless network.
2. The apparatus of claim 1, further comprising:
 - a decryption unit configured to decrypt a reply message received from the radio, the reply message encrypted with the first encryption key.
3. The apparatus of claim 2, further comprising:
 - a protocol management unit configured to convey the reply message to a host device.
4. The apparatus of claim 3, further comprising:
 - a selector configured to select between the encryption key storage units as input to the encryption unit and decryption unit.
5. The apparatus of claim 4, further comprising:
 - a device control unit configured to aid the selector in the selection between the encryption key storage units.
6. The apparatus of claim 5 wherein the second encryption key is symmetric.
7. The apparatus of claim 6 wherein the first encryption key is symmetric.
8. The apparatus of claim 7 wherein the second encryption key is a peripheral device encryption key.

1 9. The apparatus of claim 8 wherein the first encryption key is a host device
2 encryption key.

1 10. The apparatus of claim 9 wherein the peripheral device encryption key is
2 received from human input to the host device.

1 11. The apparatus of claim 10, wherein the protocol management unit is
2 configured to convey the reply message to the host device via the
3 Universal Serial Bus protocol.

1 12. A method comprising:
2 receiving a second encryption key;
3 transmitting a message containing a first encryption key over a wireless network,
4 the message encrypted with the second encryption key.

1 13. The method of claim 12 further comprising:
2 receiving a reply message encrypted with the first encryption key.

1 14. The method of claim 13 further comprising:
2 decrypting the reply message with the first encryption key.

1 15. The method of claim 14 wherein the second encryption key is symmetric.

1 16. The method of claim 15 wherein the first encryption key is symmetric.

1 17. The method of claim 16 wherein the second encryption key is a peripheral
2 device encryption key.

1 18. The method of claim 17 wherein the first encryption key is a host device
2 encryption key.

1 19. The method of claim 18 wherein the peripheral device encryption key is
2 received from human input.

1 20. The method of claim 18 wherein the host device encryption key is stored
2 within an encryption key storage unit.

1 21. The method of claim 18 wherein the encryption key storage unit that stores
2 the host device encryption key is a read only memory.

1 22. The method of claim 21 further comprising:
2 sending the decoded reply message to a host using a Universal Serial Bus
3 interface.

1 23. A computer-readable medium encoded with data and instructions, the data
2 and instructions causing an apparatus executing the instructions to:
3 receive a second encryption key;
4 transmit a message containing a first encryption key over a wireless network, the
5 message encrypted with the second encryption key.

1 24. The computer-readable medium of claim 23, the instructions further
2 causing an apparatus executing the instructions to:
3 receive a reply message encrypted with the first encryption key.

1 25. The computer-readable medium of claim 24, the instructions further
2 causing an apparatus executing the instructions to:
3 decode the reply message with the first encryption key.

1 26. The computer-readable medium of claim 25 wherein the second
2 encryption key is symmetric.

1 27. The computer-readable medium of claim 26 wherein the first encryption
2 key is symmetric.

1 28. The computer-readable medium of claim 27 wherein the second
2 encryption key is a peripheral device encryption key.

1 29. The computer-readable medium of claim 28 wherein the first encryption
2 key is a host device encryption key.

1 30. The computer-readable medium of claim 29 wherein the peripheral device
2 encryption key is received from human input.

1 31. The computer-readable medium of claim 29 wherein the host device
2 encryption key is stored within an encryption key storage unit.

1 32. The computer-readable medium of claim 29 wherein the encryption key
2 storage unit that stores the host device encryption key is a read only
3 memory.

1 33. The computer-readable medium of claim 32, the instructions further
2 causing an apparatus executing the instructions to:
3 sending the decoded reply message to a host using a Universal Serial Bus
4 interface.

1 34. An apparatus comprising:
2 means for receiving a second encryption key;
3 means for transmitting a message containing a first encryption key over a wireless
4 network, the message encrypted with the second encryption key.

1 35. The apparatus of claim 34 further comprising:
2 means for receiving a reply message encrypted with the first encryption key.

1 36. The apparatus of claim 35 further comprising:
2 means for decoding the reply message with the first encryption key.

1 37. The apparatus of claim 36 wherein the second encryption key is
2 symmetric.

1 38. The apparatus of claim 37 wherein the first encryption key is symmetric.

1 39. The apparatus of claim 38 wherein the second encryption key is a
2 peripheral device encryption key.

- 1 40. The apparatus of claim 17 wherein the first encryption key is a host device
2 encryption key.
- 1 41. The apparatus of claim 40 wherein the peripheral device encryption key is
2 received from human input.
- 1 42. The apparatus of claim 41 further comprising:
2 means for storing the host device encryption key.
- 1 43. The apparatus of claim 42 further comprising:
2 means for storing the peripheral device encryption key.
- 1 44. The apparatus of claim 43 further comprising:
2 means for decrypting received messages.

45. The apparatus of claim 44 further comprising:

means for encrypting messages to be transmitted.

46. The apparatus of claim 45 further comprising:

means for sending the decoded reply message to a host using a Universal Serial
Bus interface.

47. An apparatus comprising:

a first encryption key storage unit configured to contain a first encryption key;

a radio configured to receive a message over a wireless network from a host, the
message encoded with the first encryption key and containing a second
encryption key;

a decryption unit configured to unencrypt the message with the first encryption
key;

at least one temporary key storage unit configured to store the second encryption
key.

48. The apparatus of claim 47, further comprising:

an encryption unit configured to encrypt a reply message with the second
encryption key.

49. The apparatus of claim 48, wherein the radio is further configured to

receive data messages over the wireless network from the host, the data
message encoded with the second encryption key.

50. The apparatus of claim 49, further comprising:

a selector configured to select between the encryption key storage units as input to
the encryption unit and decryption unit.

51. The apparatus of claim 50, further comprising:

a device control unit configured to aid the selector in the selection between the encryption key storage units.

52. The apparatus of claim 51, further comprising:

a protocol management unit configured to convey the data message to a peripheral device.

53. The apparatus of claim 52, wherein the protocol management unit is configured to convey the data message to a peripheral device via the Universal Serial Bus protocol.

54. The apparatus of claim 53 wherein the first encryption key is symmetric.

55. The apparatus of claim 54 wherein the second encryption key is symmetric.

56. The apparatus of claim 54 wherein the first encryption key is a peripheral device encryption key.

57. The apparatus of claim 56 wherein the second encryption key is a host device encryption key.

58. A method comprising:

receiving a message over a wireless network from a host, the message encoded with a first encryption key and containing a second encryption key; decrypting the message using the first encryption key, extracting the second encryption key.

59. The method of claim 58 further comprising:

storing the second encryption key in an encryption key storage unit.

60. The method of claim 59 further comprising:

encrypting messages sent to the host with the second encryption key.

61. The method of claim 60 wherein the first encryption key is symmetric.

- 1 62. The method of claim 61 wherein the second encryption key is symmetric.
- 1 63. The method of claim 62 wherein the first encryption key is a peripheral
2 device encryption key.
- 1 64. The method of claim 63 wherein the second encryption key is a host
2 device encryption key.
- 1 65. The method of claim 64 wherein the encryption key storage unit is a
2 register.
- 1 66. The method of claim 65 wherein the encrypted messages sent to the host
2 are received through a Universal Serial Bus interface.
- 1 67. A computer-readable medium encoded with data and instructions, the data
2 and instructions causing an apparatus executing the instructions to:
3 receive a message over a wireless network from a host, the message encoded with
4 a first encryption key and containing a second encryption key;
5 decrypt the message using the first encryption key, extracting the second
6 encryption key.
- 1 68. The computer-readable medium of claim 67, the instructions further
2 causing an apparatus executing the instructions to:
3 store the second encryption key in an encryption key storage unit.
- 1 69. The computer-readable medium of claim 68, the instructions further
2 causing an apparatus executing the instructions to:
3 encrypt messages sent to the host with the second encryption key.
- 1 70. The computer-readable medium of claim 69 wherein the first encryption
2 key is symmetric.
- 1 71. The computer-readable medium of claim 70 wherein the second
2 encryption key is symmetric.

- 1 72. The computer-readable medium of claim 71 wherein the first encryption
2 key is a peripheral device encryption key.
- 1 73. The computer-readable medium of claim 72 wherein the second
2 encryption key is a host device encryption key.
- 1 74. The computer-readable medium of claim 73 wherein the encryption key
2 storage unit is a register.
- 1 75. The computer-readable medium of claim 76 wherein the encrypted
2 messages sent to the host were received through a Universal Serial Bus
3 interface.
- 1 76. An apparatus comprising:
2 means for receiving a message over a wireless network from a host, the message
3 encoded with a first encryption key and containing a second encryption
4 key;
5 means for decrypting the message using the first encryption key, extracting the
6 second encryption key.
- 1 77. The apparatus of claim 76 further comprising:
2 means for storing the first encryption key.
- 1 78. The apparatus of claim 77 further comprising:
2 means for storing the second encryption key.
- 1 79. The apparatus of claim 78 further comprising:
2 means for encrypting messages sent to the host with the second encryption key.
- 1 80. The apparatus of claim 79 wherein the first encryption key is symmetric.
- 1 81. The apparatus of claim 80 wherein the second encryption key is
2 symmetric.

- 1 82. The apparatus of claim 81 wherein the first encryption key is a peripheral
2 device encryption key.
- 1 83. The apparatus of claim 82 wherein the second encryption key is a host
2 device encryption key.
- 1 84. The apparatus of claim 83 wherein the means for storing the second
2 encryption key is a register.
- 1 85. The apparatus of claim 84 wherein the encrypted messages sent to the host
2 were received through a Universal Serial Bus interface.